NSC shall provide overall policy direction for the Information Security Program.

(b) *Administrator of General Services.* The Administrator of General Services is responsible for implementing and monitoring the Information Security Program established under E.O. 12356. In accordance with E.O. 12356, the Administrator delegates the implementation and monitorship functions of the Program to the Director of the ISOO.

(c) *Information Security Oversight Office*—(1) *Composition.* The ISOO has a full-time director appointed by the Administrator of General Services with approval of the President. The Director has the authority to appoint a staff for the office.

(2) *Functions.* The Director of the ISOO is charged with the following principal functions that pertain to the Department of Defense:

(i) Oversee DoD actions to ensure compliance with E.O. 12356 implementing directives, for example, the ISOO Directive No. 1 and this part;

(ii) Consider and take action on complaints and suggestions from persons within or outside the government with respect to the administration of the Information Security Program;

(iii) Report annually to the President through the NSC on the implementation of E.O. 12356;

(iv) Review this Regulation and DoD guidelines for systematic declassification review; and

(v) Conduct on-site reviews of the Information Security Program of each DoD Component that generates or handles classified information.

(3) *Information Requests.* The Director of the ISOO is authorized to request information or material concerning the Department of Defense, as needed by the ISOO in carrying out its functions.

(4) *Coordination.* Heads of DoD Components shall ensure that any significant requirements levied directly on the Component by the ISOO are brought to the attention of the Director of Security Plans and Programs, ODUSD(P).

§159a.92 Department of Defense.

(a) *Management Responsibility.* (1) The DUSD(P) is the Senior DoD Information Security Authority having DoD-wide authority and responsibility to ensure effective and uniform compliance with and implementation of E.O. 12356 and its implementing ISOO Directive No. 1. As such, the DUSD(P) shall have primary responsibility for providing guidance, oversight and approval of policy and procedures governing the DoD Information Security Program. The DUSD(P) or his designee may approve waivers or exceptions to the provisions of this part to the extent such action is consistent with E.O. 12356 and ISOO Directive No. 1.

(2) The heads of DoD Components may approve waivers to the provisions of this part only as specifically provided for herein.

(3) The Director, NSA/Chief, Central Security Service, under 32 CFR part 159, is authorized to impose special requirements with respect to the marking, reproduction, distribution, accounting, and protection of and access to classified cryptologic information. In this regard, the Director, NSA, may approve waivers or exceptions to these special requirements. Except as provided in §159a.6 the authority to lower any COMSEC security standards rests with the Secretary of Defense. Requests for approval of such waivers or exceptions to established COMSEC security standards which, if adopted, will have the effect of lowering such standards, shall be submitted to the DUSD(P) for approval by the Secretary of Defense.

§159a.93 DoD components.

(a) *General.* The head of each DoD Component shall establish and maintain an Information Security Program designed to ensure compliance with the provisions of this part throughout the Component.

(b) *Military Departments.* In accordance with 32 CFR part 159 the Secretary of each Military Department shall designate a Senior Information Security Authority who shall be responsible for complying with and implementing this part within the Department.

(c) *Other Components.* In accordance with 32 CFR part 159, the head of each other DoD Component shall designate a Senior Information Security Authority who shall be responsible for complying